

EXHIBIT B



November 4, 2013

Mr. Felix Sterling
Legal Counsel
Trend Micro
10101 N. De Anza Blvd.
Cupertino, CA 95014

Re: Claims Chart per Patent Infringement Notice

By US Mail service

To assist you in your evaluation, please note the additional product names included in this letter. By this letter, we would like to ensure that you are informed that Trend Micro is offering products and services, namely InterScan Messaging Security, Email Encryption, ScanMail™ Suite with optional data loss prevention, Messaging and Collaboration Security, Trend Micro Security as a Service, Hosted Email Encryption that we believe infringe certain patents owned by RPost. We ask that you review RPost's patents and compare them to your products and services.

The above identified products and services are electronic messaging and business management servers/platforms/applications which perform certain functions taught by RPost's patents. For example, the above identified products and services allow electronic messages to be tracked with records generated regarding the receipt, opening, and/or failure of the electronic messages, and/or outbound message content to be scanned with certain functions performed on the message based on content and server policy settings. RPost's numerous patents cover these and many other features. RPost's patents have been proven to be robust, with several emerging unscathed from re-examination and surviving attacks of invalidity in Federal Courts.

Attached to this letter is a claim charts identifying selected claims of certain patents and your infringing conduct. Please note, these claim charts are simply examples of your infringement and are by no means exhaustive. It is likely that your products and services are infringing other claims of RPost's patents. A full list of RPost's patents may be found at <http://www.rpost.com/about-rpost/intellectual-property/patents>.

We would like to discuss with you a business resolution to this matter in the next two weeks. We believe it is worth your time to have a discussion with our team in light of the value being received by the practice of RPost's patented technology. Please consider the value of your use of RPost's patents, the adverse effects of having to remove the covered features from use, and your cost to compensate RPost for past damages. Please also consider that RPost practices its patents and your continued willful infringement of its patents may result in trebled damages of RPost's lost profits.

To be clear, no one has rights to use RPost's patented technology without the express written permission of RPost. If you choose not to work out a business resolution to this matter in the next



two weeks, we request that you immediately cease and desist from manufacture, use, or offer for sale RPost's patented technology through your products and services that contain RPost's patented technology.

We look forward to hearing from you shortly.

Sincerely,

Ray Owens
Legal Affairs
RPost
legal@rpost.com

Preliminary Summary Analyses

A preliminary summary analysis of some patents follows. This summary is meant to provide you with a sample from RPost's patents and does not limit RPost's right to assert infringement to any of its patents. The language in the preliminary summary analysis is provided for discussion purposes and is not provided to define of terms in the patents that might otherwise be defined in a Markman hearing.

System and method for verifying delivery and integrity of electronic messages

US Patent 8,504,628 Claim 30	Preliminary Summary Analysis
A system for transmitting a message from a sender to a recipient, comprising:	The above identified outbound content filtering products/services transmit a sender's data/message to recipients:
a server configured to receive a message from a sender, the server being remote from a recipient of the message,	The above mentioned outbound content filtering products/services are set up as servers, remote from the recipients, configured to receive email, documents, and files.
the server also being programmable using software commands to determine if there is a particular indication present in the message that identifies the message as requiring special processing before the message is transmitted to the recipient,	The above mentioned outbound content filtering products/services can be customized and configured using software commands to inspect message content to identify specific content, flags, metadata, or combinations of data in sent message, for example, the content engine performs deep content inspection on email traffic at the email gateway, providing full visibility of: message headers, senders and recipients, subject lines, message bodies. If the particular indications, such as the word "encrypt" in the subject line, the "important" flag in the headers, urgent flags, or other administrator-configured content identification policies are present, the above mentioned outbound content filtering products/services then flag the message as requiring special processing before the message is transmitted to the recipient.



to transmit the message from the server to the recipient through a first route if the message lacks the particular indication,	The above mentioned outbound content filtering products/services transmit the message normally, on the first route, if the message does not have any of the particular indications; for example, if the message does not contain the content that the software commands are looking for to trigger special processing such as encryption, content redaction, quarantine, or retention.
and to process the message in accordance with the particular indication if the particular indication is present.	With the above mentioned outbound content filtering products/services, if the particular indication is present, then the message is processed in accordance with the software command rules associated with that particular indication. For example, if the message contains the content that the software commands are looking for, such as content or other flags to encrypt, content or content patterns flagged to redact/quarantine, then the software commands perform the indicated special processing such as encryption, content redaction, quarantine, or retention.

System and method for verifying delivery and integrity of electronic messages

US 8,224,913 Claim 1	Preliminary Summary Analysis
A method of transmitting a message from a sender to a recipient through a server acting as a Mail Transport Agent, including the steps at the server of:	The above identified products/services transmit a sender's data/message to recipients using a server that functions as a mail transport agent ("MTA").
transmitting the message to the recipient's Mail Transport Agent in a protocol dialog selected from a group consisting of the selected one of the SMTP and ESMTP protocols;	The MTA server sends electronic messages to a recipient's MTA using standard email protocols such as Simple Mail Transport Protocol (SMTP) or Extended Simple Mail Transport Protocol (ESMTP).
and recording at the server some portion of the selected one of the SMTP and ESMTP protocol dialog between the server and the recipient through the server	The MTA server creates and stores a report of each transmission, with the report including a portion of the SMTP/ESMTP protocol dialog from each transmission. For example, the MTA server records protocol dialog indicating that the recipient's MTA server was contacted and the sender's message was delivered.
including those portions of the selected one of the SMTP and ESMTP protocol dialog between the server and the recipient in which the receiving Mail Transport Agent accepts	The MTA server records at least a portion of the SMTP protocol dialog that indicates the mail transport agent server associated with the recipient email address domain has accepted the transmitted message, by for example, recording the "250 OK" record.
or declines delivery of the transmitted message.	If the message is not accepted by the mail transport agent server associated with the recipient email address domain, the MTA server records a portion of the mail transport protocol dialog that indicates



	the delivery of the message was declined, by for example, recording a "550" error code in the report.
--	-------------------------------------------------------------------------------------------------------

US 8,209,389 Claim 7	Preliminary Summary Analysis
A system for transmitting a message through an electronic mail system from an originating processor to a recipient processor and providing proof of receipt of the message by the recipient process, comprising:	The above identified products and services transmit a sender's data/message to recipients from an originating processor to a recipient processor, and providing a record of receipt of the message.
a server displaced from the originating processor, the server capable of being configured by software commands to:	The server is separate from the originating processor.
receive a message from the originating processor and to transmit the message to the recipient processor,	The server receives a message from the originating processor and transmits the sender's message to the recipient server/processor
receive an indication of receipt of the message from the recipient processor and a mail transport protocol dialog generated by the electronic mail system during transmission of the message from the server to the recipient processor,	As part of the process of transmitting the message to the recipient, the server receives a portion of the mail transport protocol dialog generated during transmission. For example, the server receives a mail transport protocol dialog that indicates the delivery of the message was declined, by for example, recording a "550" error code. The server also receives an indication of receipt of the message by the recipient, for example, after the recipient clicks a link in a received email, an image is transmitted via web protocols to the recipient web browser or email client, and the IP address of the recipient computer that had the image display in the recipient's browser is recorded by the server, the IP address information being part of the data transport dialog.
generate a first information including the indication of receipt of the message from the recipient processor and at least a portion of the mail transport protocol dialog generated by the electronic mail system during transmission of the message from the server to the recipient processor.	The server creates a report (a first information) that includes fields of indication of delivery, failure, opening, of the message, and the report includes some portion of information in the data transport dialog as noted above, such as the IP address and/or timestamp, hard or soft bounce server dialog excerpt, or sender/recipient address.

US 8,468,199 Claim 1	Preliminary Summary Analysis
A method of transmitting a message from a sender to a recipient through a server displaced from the recipient, the steps at the server comprising:	The above identified products and services transmit a sender's message/image to recipients through servers that are not at the recipient location.
receiving the message at the server from the sender;	The server receives a message from a sender.
transmitting the message to the recipient;	The server transmits the message/image via data transport protocol to the email client or web browser at the recipient.



receiving at the server at least a portion of a data transport protocol dialog generated during transmission of the message from the server to the recipient;	The server, as part of the process of transmitting the message via data transport protocol to the recipient, receives portions of the data transport protocol generated during the transmission of the document from the server (web server) to the recipient's web browser, the portion of the data transport protocol including for example, the IP address of the recipient web browser.
and receiving at the server from the recipient an indication of the failure to deliver the message to the recipient;	The server receives an indication of the failure to deliver the document to the recipient web browser or recipient email server by determining whether the data transmission (data comprising the message transferred to the web browser or email server of the recipient) has been interrupted or completed, failure or non-failure.
forming at the server a first information from the at least a portion of the data transport protocol dialog and the indication of the failure to deliver the message by the recipient;	The server creates a first information, a completion report that includes a record of the document transmission information, the completion report includes a representation of the indication of failure, which can also be an indication of non-failure, of the transmission, by indicating for example, message opened/viewed/delivered, and the first information has relied upon the information obtained from the data transport protocol dialog to make the determination of failure or non-failure of the message transmission.
and transmitting, before any authentication of the message, a copy of the first information to the sender from the server.	This first information is made available to the sender via a completion report transmitted to the sender via email, web access and/or web transmission from storage at the server.

To the extent that you make or offer messaging services that track delivery and/or opening, record an encrypted reply, or use an HTML attachment to facilitate the secure messaging process, we recommend you also review the following patents: US 8,468,198 Claim 32, 40, 41, 42; US 7,966,372 Claim 16; US 7,660,989 Claim 1; and US 8,484,706 Claim 21.

IV. List of Patents

RPost Communications Limited, RMail Limited, RPost UK Limited, and RPost Holdings Inc. Patent Coverage by Country with Patent Number(s):

AU Australia 2003224616; 706661. AT Austria EP 1 476 995 B1. BE Belgium EP 1 476 995 B1. CA Canada 2234454. CH Switzerland EP 0 760 565 B1; EP 1 476 995 B1; EP 1 570 615 B1. CN China ZL 01814748.8. DE Germany EP 1 476 995 B1; EP 1 570 615 B1. DK Denmark EP 1 476 995 B1. ES Spain EP 1 476 995 B1. FR France EP 1 476 995 B1; EP 1 570 615 B1. IN India 245930 of 2005; 239568 of 2003; 237783 of 2004. IE Ireland EP 1 476 995 B1; EP 1 570 615 B1. IT Italy EP 1 476 995 B1. JP Japan 5256358. KR Korea 10-0604630-0000; 10-1029030-0000. LU Luxembourg EP 1 476 995 B1; EP 1 570 615 B1. MX Mexico 255062. NL Netherlands EP 1 476 995 B1; EP 1 570 615 B1. UK United Kingdom EP 0 760 565 B1; EP 1 476 995 B1; EP 1 570 615 B1. US United States Patent Numbers: 6182219c1; 6571334c2; 7240199; 7660989; 7698558; 7707624; 7865557; 7886008; 7966372; 8161104; 8209389;



www.rpost.com

RPost Holdings Inc.

8224913; 8275845; 8468199; 8468198; 8478981; 8484706; 8504628. PT Portugal EP 1 476 995 B1. SE Sweden EP 1 476 995 B1.

RPost Communications Limited and RPost Holdings Inc. Published US Patent Applications: 20130117387; 20130086654; 20130086186; 20120303956; 20120278417; 20120265829; 20110246588; 20110145889; 20110106897; 20110072077; 20100250691; 20100235892; 20100217969; 20090217028; 20070174402; 20060112165; 20050198511; 20050021963; 20040230657; 20040221014; 20030172120; and 20020144154. RPost also holds additional US Patent Applications that have yet to be published. Additional RPost patents can be found online at <http://www.rpost.com/about-rpost/intellectual-property/patents> where RPost lists its 46 patents by patent number. Refer to list of patent application numbers at the end of this letter and patents and patent applications listed at www.uspto.gov under inventor name "Tomkow".